IT Security Procedural Guide: Conducting Penetration Test Exercises CIO-IT Security-11-51

Revision 6

November 25, 2022

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – April 30, 2012		
1	Bo Berlas	Clarified guidance relating to performance of penetration testing against development environments.	Penetration testing shall occur against production environments to ensure testing activities reflect the risks of the system under review.	8
		Revision 2 – December 11, 2014		
1	Bo Berlas	Changed requirement for penetration testing from ALL systems (i.e., FIPS PUB 199 Low, Moderate and High) to FIPS PUB 199 Low and Moderate Internet accessible systems and All FIPS PUB 199 High.	Focuses penetration testing activities at areas of greatest risk. Aligns with updated requirements in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk".	Pages 4 and 8
2	Bo Berlas	Changed references to Office of the Senior Agency Information Security Officer (OSAISO) and Senior Agency Information Security Officer (SAISO) to Office of the Chief Information Security Officer (OCISO) and Chief Information Security Officer (CISO)	Administrative to reflect changes in office name and CISO title as a result of IT and IT Security consolidation.	Numerous
3	Blanche Heard	Updated to reflect references to comply with ADM O 5440.667	Organization titles and responsibilities	Numerous
		Revision 3 – December 1, 2015		
1	Bo Berlas	Updated Reporting Template and associated references	Updated to reflect changes to NIST SP 800-53 Rev 4 and reflect process updates	Pages 9 and 20
2	William Salamon	Updated Reporting Template, Rules of Engagement Template, and updated several sections	Reflect changes to OWASP, NIST SP 800-15 recommendations, incorporate cloud computing concepts, and other process updates	Pages 11-12, 16-17, 21-22
		Revision 4 – January 18, 2018		
1	Dean/ Feliksa/ Klemens/ Newsome	Revised to reflect current GSA processes and procedures for conducting penetration tests.	Revised to reflect how GSA conducts penetration tests based on Federal policies, NIST controls with GSA parameters, and GSA processes and procedures. Updated to current guide structure and format.	Throughout
		Revision 5 – July 24, 2020		
1	Armando Quintananieves/ Angela Christian/ Raja Hayat/ Branndon Dean	Primary changes: • Expanded the types of pen tests listed. • Clarified pen test approaches.	Revised to reflect current GSA processes and procedures for conducting penetration tests in different environments.	Throughout

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		• Added section on specific pen tests GSA conducts and their applicability. • Added section on responsibilities for system and pen test roles. • Added an Appendix with GSA A&A Penetration Test Minimum Requirements. • Modified formatting and style to latest guidance, including 508 compliance.		
		Revision 6 – November 25, 2022		
1	Jerod Weaver	• Added new API and Container focused Pen tests. • Updated the minimum requirements table to remove PTES from non-applicable test types.	Revised to reflect current GSA guidance and requirements for various environments.	Various
2	McCormick	• Reviewed and edited guide for formatting, style, and content changes.	Updated to current guide formatting and style.	

Approval

IT Security Procedural Guide: Conducting Penetration Test Exercises, CIO-IT Security 11-51, Revision 6, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.

Table of Contents

Notes:

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a webpage or document listed in Section 1.4. For example, Google Forms, Google Docs, and websites will have links.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document**.**

1 Introduction

A penetration test is an authorized simulation of a cyberattack which is used to identify security weaknesses by way of technical flaws, misconfigurations, vulnerabilities, and/or business logic. A penetration tester will attempt to exploit weaknesses to gain access, modify functionality, and/or corrupt the business logic of the target system without creating additional risk to the agency or organization. The penetration tester will attempt to perform activities of a malicious actor; however, such activities will be conducted ethically and with the permission of the General Services Administration (GSA) Office of the Chief Information Security Officer (OCISO) prior to execution.

A penetration test exercise supports the overall risk management process by identifying security risks and demonstrating exploitability of findings that may not be readily apparent when performing a security review. A penetration test can be performed with or without knowledge of the system and involves the execution of a scenario and use cases that focus on violating technical, administrative, and management controls to gain access to the system or data.

Penetration tests can be used to verify and prove scan results that are false positives or false negatives. Penetration tests, as opposed to vulnerability scans, should not have false positive findings since they only report on found vulnerabilities. Penetration tests, while capable of verifying or proving a specific false negative finding, are not exhaustive and therefore cannot prove there are no vulnerabilities to a system. The test processes described in this document are used for measuring, evaluating, and testing the security posture of a system, but test findings should not be used to the exclusion of other security processes (e.g., architecture analyses, configuration checks).

1.1 Purpose

This procedural guide provides guidance for performing penetration test exercises against GSA applications, infrastructure, and systems. The GSA Chief Information Officer (CIO), in Chapter 2 of GSA Order CIO 2100.1, GSA Information Technology (IT) Security Policy, identifies GSA Federal employees and contractors with significant security responsibilities. This guide provides those personnel identified in CIO 2100.1 and other IT personnel involved in penetration testing exercises on GSA IT resources an independent, repeatable framework for conducting penetration test activities.

1.2 Scope

The requirements outlined within this guide apply to any internal or external organizations involved in penetration testing of GSA systems and data.

1.3 Policy

GSA Order CIO 2100.1 contains the following statements regarding penetration testing.

CHAPTER 3: POLICY FOR IDENTIFY FUNCTION

4. Risk Assessment.

b. All Internet accessible information systems, and all FIPS 199 High impact information systems are required to complete an independent penetration test (or 'pentest') and provide a Penetration Test Report documenting the results of the exercise as part of the A&A package. In addition, these same systems must complete penetration tests annually. "Independent" testing means the testers are free from any perceived or actual conflicts of interest regarding the development, operation, or management of the information system(s) targeted by the penetration test.

c. Independent vulnerability testing including penetration testing and system or port scanning conducted by a third-party, such as the GAO and other external organizations, must be specifically authorized by the AO and supervised by the ISSM.

1.4 References

Federal Laws, Standards, Regulations, and Publications

- Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115, "Technical Guide to Information Security Testing and Assessment"
- NIST SP 800-145, "The NIST Definition of Cloud Computing"
- NIST National Vulnerability Database (NVD), Common Vulnerability Scoring System (CVSS)

GSA Directives, Policies, and Guidance

The GSA policies listed below are available on the GSA.gov Directives Library page.

- GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy"

The GSA CIO-IT Security Procedural Guide listed below is available on the internal GSA InSite IT Security Procedural Guides page.

- CIO-IT Security-01-02, "Incident Response"

Other Applicable Sources:

- Common Vulnerability Scoring System (CVSS-SIG), CVSS v3.1: Specification Document
- Open Web Application Security Project (OWASP), OWASP Serverless Top 10
- OWASP, OWASP Top Ten
- OWASP, OWASP Web Security Testing Guide v4.1 (WSTGv4.1) - OWASP has developed v4.2, however GSA has not yet moved to that version
- Penetration Testing Execution Standard (PTES) Technical Guidelines, PTES-TG
- SANS, CWE/SANS TOP 25 Most Dangerous Software Errors

2 Penetration Testing Overview

A penetration test is an authorized simulation of a cyberattack which is used to identify security weaknesses by way of technical flaws, misconfigurations, vulnerabilities, and/or business logic, with or without knowing the inner workings of the system. NIST SP 800-115 describes two primary types of penetration testing: external and internal testing.

External security testing offers the ability to view the environment's security posture as it appears outside the security perimeter, usually as seen from the Internet, with the goal of revealing vulnerabilities that could be exploited by an external attacker.

In internal security testing, assessors work within the security perimeter, assuming the identity of a trusted insider or an attacker who has penetrated the perimeter defenses. This testing can reveal exploitable vulnerabilities and demonstrates the potential risk to the organization or agency. Internal security testing also focuses on system-level security and configurations including application and service configuration, authentication, access control, and system hardening.

2.1 Types of Penetration Tests

In general, there are 14 types of penetration tests.

1. **Network Penetration Tests**
   Network penetration testing is used to evaluate the susceptibility of systems to network attacks by identifying and exploiting weaknesses found in networks, hosts, and devices to help assess the level of risk posed by specific vulnerabilities in accordance with PTES and PTES-TG.
2. **Web Application Penetration Tests**
   Web application security testing involves an active analysis and exploitation of the web application for any weaknesses, technical flaws, or vulnerabilities in accordance with the OWASP WSTGv4.1.
3. **Software or Application Penetration Tests (includes Mobile Application and Application Programming Interface [API] testing)**
   Software application testing evaluates the security of internal software applications using white box testing during the developmental phase to find and remediate system flaws in the application prior to deployment. Software testing generally utilizes reverse engineering and its techniques.
4. **Social Engineering Tests**
   Social engineering testing evaluates the human aspect of the organization or agency using email phishing or other social or non-technical means to test the organizational security awareness training program.
5. **Wireless Network Penetration Tests**
   Wireless network penetration testing evaluates the susceptibility of the agency's wireless network components, including but not limited to access points, Internet of

Things (IoTs) devices, and hosts. It helps to assess the level of risk posed by specific vulnerabilities in accordance with PTES and PTES-TG.

6. **Physical Penetration Tests**
   The primary objective for a physical penetration test is to measure the strength of existing physical security controls and uncover their weaknesses before bad actors can discover and exploit them.

   Physical penetration testing, or physical intrusion testing, will reveal real-world opportunities for malicious insiders or bad actors to compromise physical barriers (e.g., locks, sensors, cameras, mantraps) and obtain unauthorized physical access to sensitive areas leading up to data breaches and system/network compromise.

7. **Incident Response (IR) Penetration Tests**
   IR penetration testing is performed at the request of the Incident Response Federal Lead or Information Security (IS) Division Directors with approval from the GSA CISO in response to an identified incident on an external facing Web Application. Incident response penetration tests utilize SANS Top 25 Most Dangerous Software Errors and can be authenticated or unauthenticated. The test can include specific exploits observed during the incident. Additionally, internal testing may be conducted to determine the extent of the incident.

8. **Phishing**
   GSA Security Operations Division (SecOps) regularly performs phishing testing across the agency. GSA currently uses CoFense PhishMe, but other tools can be used as well. Phishing emails are sent to randomly selected GSA federal employees and contractors. By request from the associated Federal Information Security Modernization Act (FISMA) systems, the Information System Security Manager (ISSM)/Information System Security Officer (ISSO), or GSA CISO, a phishing attack can be designed and carried out on GSA end users and GSA admin role users. At the end of the attack, a report will evaluate the attack, identifying users who were successfully phished.

9. **Network Stress Tests**
   Stress testing evaluates whether a computer, application, device, or the entire network can withstand high loads and remain operational. A stress test can simulate an adverse condition that takes a system down or at least decreases its performance. These types of tests are recommended for any component on the GSA network but not recommended for any Amazon Web Services (AWS) component without prior AWS approval.

10. **Cloud Penetration Testing**
    Cloud penetration testing takes place in the cloud environment. During this process the penetration tester will review cloud security configurations as well as systems, web apps, and other components associated with the cloud environment.

11. **Serverless Penetration Testing**
    Applications that run on serverless providers, such as AWS Lambda and Google Cloud Functions use serverless penetration testing. This type of testing focuses on vulnerabilities from a serverless environment perspective, such as Hypertext Transfer

Protocol (HTTP) APIs, messages, cloud storage, and IoT devices, including protocols used for these components. Testing is performed based on the OWASP Serverless Top 10, taking into consideration the attack surface and overall system complexity.

12. **Red Team/Blue Team (Purple Team) Testing**
    Purple teaming is a security methodology whereby red and blue teams utilize attack (red) and defend (blue) cyber capabilities to enhance security knowledge and inform security improvements through continuous feedback and knowledge transfer.

13. **Open-Source Intelligence (OSINT) Assessment**
    OSINT is a highly diverse form of unclassified intelligence data collected from overt and covert sources to be assessed and used to make proactive decisions about imminent risks facing the organization at a tactical and strategic level.

    Active OSINT collection may include active scanning for sensitive domain data on the darknet, as well as listening for darknet chatter of upcoming attacks which will assist the agency in long-term strategic decision making. Passive OSINT collection may include techniques such as using web crawlers (e.g., Google search indexing engine) to identify accidental data/vulnerability exposure on the Internet and organizational threat discussions on social media.

14. **Business Logic Assessment (BLA)**
    BLAs are manual assessments of application security weaknesses that cannot be tested effectively in an automated manner. BLAs consist of reviewing internal policies and procedures and applying those to an application's business logic to identify and limit risk to the agency.

2.2 Penetration Testing Approaches

As part of planning the penetration test exercise, the test team has to determine the level of access required for the exercise. The penetration tester acts like an attacker and attempts to find and exploit vulnerabilities within the defined scope and boundaries granted by the Rules of Engagement (RoE). In many cases, the penetration tester will be given a valid account on the system. The following terms are used to describe penetration testing approaches: black box, gray box, and white box.

Black Box Testing

The black box testing approach assumes the penetration tester has no knowledge of the internal structure and implementation detail of the assessment object. Because an attacker will incorporate a low and slow attack strategy to avoid detection of the targeted attack, it can take months and even years for the attacker to gain enough information about the system to initiate an effective cyberattack.

Black box testing is very difficult to simulate as most penetration tests typically only last a few weeks. This type of testing is done only with CISO approval.

White Box Testing

In white box testing, the penetration tester has full, unrestricted access to the target environment including the internal structure and source code. Testing can include running test cases to check whether the system meets specification requirements. Using derived test cases, the tester exercises the test cases by providing input to the system and comparing the actual output to expected output. In this type of testing, the tester has to go beyond the user interface to test the correctness of the system.

White box testing is one of the best approaches to find errors in the development stage of a system's life cycle. In this process, deriving test cases is an important part of the test exercise. The test case design strategy should include execution of all lines of the source code and/or all available functions at least once to complete 100% code coverage during testing. Access to underline documents, network, and all levels of access is required. This type of testing is done only with IS Director or CISO approval.

At a minimum, the following information will be provided to the penetration testing team:

- Network Diagram
- System Security and Privacy Plan (SSPP)
- Full Admin Level access to internal and external interface
- List of Administrator users to both Network and Web interface
- Vulnerability Scan Data (Web/Network/Software)
- Code Coverage
  - Control Flow Testing
  - Data Flow Testing
  - Branch Testing
  - Statement Testing
  - Decision Coverage
  - Modified condition/decision Coverage
  - Prime Path Testing
  - Path Testing

Gray Box Testing

Gray box testing is GSA's Accepted Penetration Testing Standard. Gray box testing is a hybrid approach between black box and white box testing. In gray box testing, the internal structure is partially known. This often involves having access to internal data structures and algorithms for purposes of designing the test cases but performing testing at the user or black box level. Gray box testing provides many of the benefits of white box testing such as reducing the time required for information gathering while maintaining the external threat perspective.

At a minimum the following information will be provided to the penetration testing team:

- Network Diagram
- SSPP
- Accounts (Web Interface/Network): One for each role
- List of Administrator users for both Network and Web interface
- Vulnerability Scan Data (Web/Network/Software)

There are multiple factors to consider when deciding which penetration testing approach to use on a target system. The relationship between time and system exposure is important. While time is a restraint to ethical hackers, system exposure is a restraint to the non-ethical hackers. Utilizing the gray box testing approach allows ethical hackers to save time by working with developers and system administrators to understand the functionality and operation of target systems while non-ethical hackers have to spend more time researching the system in an attempt to gain similar knowledge.

2.3 Defining the Scope and Test Boundary

Properly defining the scope of the penetration test is necessary to ensure the test exercise is focused on relevant components and to safeguard against testing components that are outside of the system's authorization boundary unless authorized per the RoE. ISSMs/ISSOs and test personnel must strike a balance between performing a comprehensive set of tests and evaluating functionality and features that present the greatest risk. Any special cases or sensitivities should be carefully evaluated to prevent disruption of service prior to the start of the exercise. GSA's accepted standard scope is any interaction that is identified in the SSPP. Testing interconnections with third party entities is considered out of scope until the third party agrees to an assessment.

2.4 Vulnerability Risk Rating

Risk ratings provide GSA with a metric to calculate the associated risk of an identified vulnerability. Risk ratings are defined by the NIST CVSSv3.x based score. The penetration tester uses these risk ratings to justify the assigned severities of vulnerabilities. A penetration tester will typically use the CVSSv3.x calculation:

Attack Vector (AV): Attack Complexity (AC): Privileges Required (PR): User Interaction (UI): Scope (S): Confidentiality (C): Integrity (I): Availability (A)

Note: Vulnerability severity can deviate from NIST CVSSv3.x when directed by GSA SecOps management. For example, vulnerabilities associated with Binding Operational Directive (BOD) compliance have an elevated severity, while findings with risk mitigation implemented may have a decreased severity rating to account for risk mitigation.

2.5 Exploiting Vulnerabilities

The purpose of a penetration test is to identify risk to GSA by exploitation of potential vulnerabilities and/or other security weaknesses. Because security scan tools do not always validate the presence of a finding, scanning tools are often configured to make educated guesses about the presence of potential vulnerabilities and, in certain cases, validation requires a human to perform manual inspection and testing to confirm the finding. Actively exploiting a system is often much harder than simply identifying potential vulnerabilities. A penetration tester will utilize various open source and commercial penetration testing tools.

While the specific means and methods used to exploit vulnerabilities may vary, Section 3 defines the process which will be applied to ensure test activities are reasonable and conducted within appropriate limits.

3 GSA Penetration Tests Defined

3.1 GSA Assessment and Authorization (A&A) Penetration Test

3.1.1 Web Application Penetration Tests

The GSA A&A Web Application Penetration Test is a gray box test (unless otherwise specified with the appropriate approvals), authenticated, and covers all OWASP WSTGv4.1 controls. All external facing FISMA systems involved in the full A&A process require a GSA A&A Penetration Test. A request for an internal system Web Application Penetration Test requires approval from the ISSM, IS Directors, or GSA CISO. Penetration testing of all environments (Test/Dev/Prod) will be allowed only with approval of the IS Federal Penetration Test Lead.

3.1.2 Network Penetration Tests

The GSA A&A Network Penetration Test is only performed on FIPS High systems *or* at the request of the CISO. During this penetration test, the network side is penetration tested using PTES-TG and web applications are penetration tested using OWASP WSTGv4.1 controls. Network penetration testing can be performed from an internal or external perspective depending on the needs of the network and what is defined as the scope within the SSPP. These penetration tests are authenticated and gray box unless otherwise specified with the appropriate approval. Penetration testing of all environments (Test/Dev/Prod) will be allowed only with approval of the IS Federal Penetration Test Lead.

3.1.3 API Specific Penetration Tests

The GSA API Specific Penetration Test is performed against externally facing API endpoints. This type of testing focuses on API specific security concerns and does not include Web Application Penetration Testing. GSA API Specific Penetration testing will only be used to test API components and must be approved by the ISSM and the ISSO Support (IST) Division Director.

3.1.4 Container Specific Penetration Tests

The GSA Container Specific Penetration Test is performed against Web Applications which are hosted in containerized environments. This penetration test type is based on the OWASP WSTGv4.1 tests and is tailored to focus on potential areas of exploitation specific to containerized environments, while also excluding a small number of tests which do not provide value in these types of environments.

3.2 GSA Annual Penetration Tests

3.2.1 Ongoing Authorization (OA)

Systems in OA will receive an annual penetration test of their external URLs. Any exceptions to this rule will need the Security Operations (ISO) Division Director or CISO approval.

3.2.2 FISMA High Value Assets (HVAs)

All FISMA HVAs are required to have a full A&A Penetration Test annually.

3.2.3 FIPS 199 High Systems

All FIPS 199 High systems are required to have a full A&A Penetration Test annually.

3.2.4 FIPS 199 Moderate and Low

For FIPS 199 Moderate and Low systems not covered in Sections 3.2.1-3.2.3, GSA's annual penetration test is performed on a sampling of external interfaces as approved by the CISO. These penetration tests are unauthenticated and at a minimum shall utilize OWASP's Top 10. The GSA annual penetration test does not replace the full A&A Penetration Test requirement required for Moderate and Low systems undergoing A&A.

3.3 GSA Delta Penetration Test

GSA's Delta Penetration Test focuses on penetration testing minor changes to a web application. Delta Penetration Tests are authenticated, utilize OWASP WSTGv4.1, and are gray box. The scope is based on the changes made to the application. Delta Penetration Tests are conducted only with approval from the FISMA system ISSM/ISSO. Penetration testing of all environments (Test/Dev/Prod) will be allowed only with approval of the IS Federal Penetration Test Lead.

3.4 GSA Incident Response (IR) Penetration Test

GSA's IR Penetration Test is conducted with CISO approval and in response to a documented incident. Incident response penetration tests can be either unauthenticated or authenticated, are gray box and utilize SANS Top 25 Web Application Vulnerabilities testing methodology.

Note: All GSA penetration tests must be performed against the production environment. If the system is a new system, it will need to be placed into a pre-production ("pre-prod") environment. Test and Dev environments are not externally accessible. Any requests for penetration testing outside of the production or pre-production environment must be submitted by the ISSM and approved by CISO. This approval will then be documented and included in the penetration team's final package. Penetration testing of all environments (Test/Dev/Prod) will be allowed only with approval of the IS Federal Penetration Test Lead.

4 GSA Penetration Testing Process

GSA requires an independent penetration test on the system or system components for all Internet facing and FIPS 199 High systems.

Independent penetration test agents or teams are individuals or groups who conduct impartial penetration testing of organizational systems. Impartiality implies that penetration test agents or teams are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the system(s) that are targeted by the penetration testing exercise.

The following sections constitute a generic version of the penetration test process to be followed for network, software/application, and web application penetration testing. The test phases may be repeated as required through the process based on the scope of the exercise.

4.1 Responsibilities

A penetration test is a coordinated effort between the ISSM/ISSO, System Owner, and the Penetration Testing Team. The following lists the responsibilities of each party in conducting a penetration test.

4.1.1 ISSM/ISSO

- Initiates the penetration test request with Penetration Testing Lead
- Provides the type of penetration test to be conducted
- Identifies scope/provides SSPP
- Signs the RoE

Note: Penetration tests that fall outside of the GSA's accepted standard will be addressed with ISO Federal and Contractor leadership.

4.1.2 Penetration Test Lead

- Drafts kickoff meeting slides and RoE
- Schedules kickoff meeting
- Verifies the penetration test type
- Validates the scope
- Manages the penetration test schedule
- Assigns a penetration tester(s)
- Signs the RoE
- Circulates the RoE for signatures

4.1.3 System Owner

- Conducts system backups
- Provides penetration tester access
- Provides an acceptable penetration test window
- Whitelists the penetration test VPN

- Signs the RoE

4.1.4 Penetration Tester/Team

- Signs the RoE
- Conducts the penetration test
- Provides risk ratings and recommendations
- Validates remediations
- Prepares penetration test report

4.2 Planning Phase

A kickoff meeting must be held to share contact information and establish key points of the project timeline. The kickoff meeting typically covers the following topics:

- Key personnel points of contact
- Review of RoE document
- Define responsibilities for coordination and conduct of the Pen Test
- A manual, non-intrusive review of any relevant forms, queries, and previous vulnerability and/or penetration test reports
- Testing window's start and finish times and dates
- Final reporting process
- Signed final RoE document via electronic signature.

The kickoff meeting should include the Penetration Test Lead, System Owner, Lead Penetration Tester, and ISSM/ISSO. Key stakeholder(s) should be fully aware of the test protocol and be able to intervene when necessary.

Note: System Owners are responsible for backing up their systems prior to the start of testing. In addition, organizations may want to have their continuity of operations and disaster recovery plans in place and operational prior to testing so they are assured that system failures due to testing can be quickly and efficiently overcome.

Note: An RoE Kickoff Presentation template and additional penetration testing templates are available on the GSA InSite Forms and Aids page. Google Docs versions of all penetration testing templates are available to internal team penetration testers on a GSA Google Drive.

Prior to signing the RoE, System Owners are responsible for notifying all third parties who will be affected by the penetration testing exercise, including but not limited to:

- Cloud Services Provider(s);
- Internet Service Provider(s); and/or
- Other System Owners using the same platform.

For external penetration testing, the Penetration Testing Team is responsible for obtaining a signed RoE for penetration testing exercises on GSA systems and data and providing it to their Internet Service Provider (as necessary). Even though the client may approve this risk, it must always be clearly communicated with the Internet Service Provider.

Note: Any documentation provided to the Internet Service Provider must first be cleared by the GSA OCISO.

4.2.1 Penetration Test Scope

The penetration test scope defines what is being tested. For all penetration tests the scope must be defined and provided to the Penetration Testing Team by the ISSM/ISSO. For A&A assessments, the scope should match the boundaries defined in the SSPP. If an SSPP is not available, the Penetration Testing Team will work with the ISSM/ISSO and System Owner to outline and validate the scope of the penetration test. The scope will be reviewed and identified in the RoE.

4.3 Defining the Rules of Engagement

Penetration testing is used to identify security weaknesses including technical flaws, misconfigurations, vulnerabilities, and/or business logic. In order to minimize the potential for service disruption, damage, or loss of integrity, the OCISO IST Division provides an Assessment Penetration Test Rules of Engagement template which outlines the responsibilities and limitations of the testing team and the System Owner throughout the entire testing process. Prior to testing, the Authorization Memorandum template must be completed and signed by key personnel in order to ensure there is a common understanding of the limitations, constraints, liabilities, and considerations between the System Owner and the Penetration Testing Team throughout the GSA penetration test process.

During this process, stakeholder(s) should establish specific reporting thresholds in a manner consistent with the risk and impact of any potential vulnerability. OCISO IST Division recommends that established thresholds allow the Penetration Tester to determine the impact of vulnerability exploitation, not just the existence or presence of vulnerabilities. Knowing the potential impact and severity of individual flaws will allow developers and engineers to focus efforts on patching and fixing vulnerabilities based on their severity levels.

If the Penetration Testing Team identifies a high-risk vulnerability, the finding will be reported to the ISSO, ISSM, and System Owner. As part of this notification, the System Owner agrees to not modify the system until the end of the assessment or approval from the Penetration Testing Team. The Penetration Testing Team will work with the System Owner upon remediation(s) to validate that vulnerability findings have been resolved.

In general, the execution of a penetration test exercise involves the active exploitation of systems and information. While the objective of the penetration test is to recreate the conditions and environment that can be exploited by a bad actor, a GSA-sanctioned penetration test is a scenario designed to explore existing vulnerabilities in a controlled and deliberate manner.

Important principles of GSA penetration test exercises include but are not limited to:

- The Penetration Testing Team will not violate the scope or boundary of the Penetration Testing Exercise defined in the Rules of Engagement and the Authorization Memorandum.
- The Penetration Testing Team will not maintain persistence beyond the testing window defined in the Authorization Memorandum.
- The Penetration Testing Team will not introduce any new vulnerabilities to the target system or its components.
- The Penetration Testing Team will not modify or delete log/audit trails of a target system to clear their tracks.

Prior to testing, all personnel involved should have a common understanding of the limitations, constraints, liabilities, and indemnification considerations between the System Owner and the Penetration Testing Team throughout the penetration test. The Penetration Testing Team may attack the application which may disable account users or system services. In the case of any service interruptions, the System Owner will be responsible for resetting accounts in a timely manner so as not to restrict or extend the testing window.

4.4 Penetration Testing Authorization

Prior to commencement of penetration test activities, OCISO must review the RoE document and approve the Authorization Memorandum. Upon approval of the Authorization Memorandum, permission will be granted to specific members of the Penetration Testing Team to conduct penetration tests against GSA's assets defined in the applicable SSPP while conducting such test(s) in accordance with the rules defined in the project Rules of Engagement Document.

4.5 Test Phases

The testing process will involve four primary phases: information gathering (mapping/ reconnaissance), discovery, exploitation (attack), and documentation/reporting.

Information Gathering. After performing the necessary notifications, the Penetration Testing Team begins information gathering activities to collect data that can be used as inputs for discovering vulnerabilities. The testing phases may be repeated multiple times throughout the exercise (as required) based on the Rules of Engagement and structure of the tests assigned to the exercise.

The information gathered during the mapping/reconnaissance phase is reviewed to mark potential exploitable vulnerabilities. Information gathering is critical to understanding the attack surface and establishing the system's public footprint which includes:

- Discovering open source disclosures
- Enumerating public interfaces
- Identifying system architecture and components
- Diagramming application flow and design

- Surveying the hosting environment
- Discovering control channels

Discovery. Vulnerability discovery is the process of testing and probing system entry points for flaws that can be used to generate an error condition, raise an invalid response, monitor traffic or data, or control a key system process. Examples of these vulnerabilities include:

- Business process/logic or design flaws
  - Registration forgeries
  - Account/password reset attacks
  - Self-registration and account spoofing
  - Administrative/control channel monitoring and capture
- Development errors
  - Input validation
  - Parameter processing
  - Authentication bypass
  - Script injection
  - Privilege escalation
- Configuration flaws
  - Default accounts
  - Accessible administrative interfaces
  - Versioning/error messages
  - Unpatched services
  - Provider/peer relationship forgery
  - Open service abuse
  - Internal/shared configurations

Exploitation. During the exploitation phase, the penetration tester determines whether vulnerabilities can be exploited to gain unauthorized access to systems and/or data. The nature of this phase is largely dependent on the findings from the vulnerability discovery phase and must be conducted in accordance with the established Rules of Engagement.

During the information discovery and exploitation phases of the penetration test, testers will document penetration test findings in order to provide a record and accounting of the specific actions taken during the test for use in the final report.

Note: System Owners should be allowed viewer access to penetration test findings during the penetration test exercise but will not be authorized to remediate any of the findings until after the test window ends as defined in the RoE.

Documentation. In the documentation phase, the lead penetration tester uses the penetration test findings captured during the test to populate the "Summary of Findings" and "Detailed Findings" sections of the Penetration Test Report Template. The report will also include a summary describing the tests conducted, the findings, a severity rating based

on the risk to GSA and its interests, and related recommendations for mitigation or a technical solution.

Any security issues found during the exercise(s) will be presented to the ISSM/ISSO and System Owner with an assessment of the impact, a proposal for mitigation, or a technical solution.

4.6 Additional Considerations

Tester(s) may leverage tools and techniques employed by real attackers, including open source, custom-developed, and commercial software tools.

All penetration test exercises should focus on identifying exploitable vulnerabilities in a manner that does not affect end-users, if possible. The Penetration Testing Team should make every attempt to provide specific windows of time (e.g., maintenance windows) to avoid disruption of system usage.

Taking advantage of vulnerabilities during penetration testing can cause system instability, which can result in the corruption or loss of data as well as unintentional Denial of Service (DoS). DoS testing is not currently authorized by the GSA. However, if a DoS testing exercise is required, the OCISO IST Division will coordinate with the appropriate GSA Officials for approval.

5 Incident Response Procedures

If a reportable threat or incident is found consistent with the current CIO-IT Security-01-02, the Penetration Testing Team shall stop testing immediately and report the incident to the ISSO, ISSM, and System Owner. Testing will resume after the incident is resolved with the approval of the ISSO, ISSM, and System Owner.

6 Points of Contact

All penetration test exercises must be coordinated through the GSA OCISO. Penetration tests of internal GSA systems (inside the GSA firewall) must also be coordinated with the GSA Penetration Testing Team [iso-pentest@gsa.gov] and GSA Incident Response [gsa-ir@gsa.gov].

Appendix A. Penetration Testing Minimum Requirements Matrix

Table A-1 describes GSA's minimum requirements for penetration testing of FIPS 199 Low, Moderate, and High systems.

Table A-1. Penetration Testing Minimum Requirements Matrix

FIPS Level	A&A	Annual Pen Test	Network Pen Test	Delta Pen Test	IR Pen Test
Low	External Interfaces OWASP WSTGv4.1 Gray Box Authenticated	External Interfaces OWASP WSTGv4.1 Top Ten Gray Box Unauthenticated	N/A	ISSM or CISO Approval External Interfaces	Director or CISO requested. Based on Incident Response SANS Top 25 and/or PTES-TG
Moderate	External Interfaces OWASP WSTGv4.1 Gray Box Authenticated	External Interfaces OWASP WSTGv4.1 Top Ten Gray Box Unauthenticated	N/A	ISSM or CISO Approval External Interfaces	Director or CISO requested. Based on Incident Response SANS Top 25 and/or PTES-TG
High	Internal & External Interfaces OWASP WSTGv4.1 & PTES-TG Gray Box Authenticated	Internal and External Interfaces OWASP WSTGv4.1 & PTES-TG Gray Box Authenticated	Internal and External Interfaces	ISSM or CISO Approval External Interfaces	Director or CISO requested. Based on Incident Response SANS Top 25 and/or PTES-TG

Appendix B. Penetration Test Templates

The following templates are used in the process of conducting penetration tests at GSA. They are available on the GSA InSite IT Security Forms and Aids webpage.

Note: Google Docs versions of the penetration testing template are available for internal team penetration tests on Google Drive.

- The **Kickoff Meeting Presentation template** documents the appropriate contact information and establishes key points of the project timeline.
- The **Penetration Test Rules of Engagement template** is a required agreement that outlines the responsibilities and limitations of the testing team and the System Owner throughout the entire testing process. The document must be reviewed and approved by the OCISO IST Division prior to any penetration test exercises. It includes the authorization memorandum.
- The **Penetration Test Report template** is prepared by the OCISO IST Division. It includes information from the penetration test findings and describes the tests conducted, the findings, a severity rating based on the risk to GSA and its interests, and related recommendations for mitigation or a technical solution.

Appendix C. GSA A&A Penetration Test Detailed Minimum Requirements

This appendix describes GSA minimum requirements for A&A penetration testing.

- Web Application Penetration Testing
  - Must follow OWASP WSTGv4.1 Guidelines
  - No scenarios, all OWASP WSTGv4.1 controls must be tested against. Applicable vs. not applicable should be noted in the penetration test documentation.
- Network Penetration Testing
  - Must follow PTES-TG guidelines
  - No scenarios, all PTES-TG controls must be tested against. Applicable vs. not applicable should be noted in the penetration test documentation.
- Penetration Tests
  - External facing components must have penetration testing performed from an external perspective.
  - Only components with internal-facing-only interfaces can be penetration tested from an internal perspective.
  - Only production or pre-production environments.
  - If authentication is available, the penetration tester must perform the penetration test utilizing authentication.
  - Gray Box Penetration Testing is GSA's accepted standard.
- Reporting
  - Initial raw scan data should be retained and presented with the final report.
  - Final Report Package should include documentation of all OWASP WSTGv4.1 controls tested.
  - Final Report should include a screenshot of each finding
  - Final report should include finding severity
  - Final report should include tool(s) used to identify finding
  - Final report should include a description of each finding.
  - Final report should include all findings before remediation.
    - Remediation can occur only after the file report has been distributed to IST management.
    - Once a finding is remediated, the final report should be updated identifying the finding as remediated.
      - The original finding should not be removed from the report
    - False positive findings should be identified as false positives and not removed from the final report.
      - False Positive findings should include justification for the false positive reclassification.
      - False positive findings are subject to approval from GSA IST and ISO management with final approval from GSA CISO.
  - Each updated final report should be identified by indicating an updated version to the back of the report. (Example 02 Penetration Test Report v1.0, 02 Penetration Test Report v1.1, and so on).

- Validation
    - Once a finding is remediated, the Systems Owner/ISSO/ISSM/or appointed contact should contact the Penetration Testing Team for validation. During the assessment period, the team will update the Penetration Testing Report.
        - Once the assessment period is complete, an email will be sent confirming validation. Any further updates will need to be updated in the system's Plan of Action and Milestones (POA&M).